NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

Visualization and Controls Program
Peer Review 2006
Protocol Authentication

Jeff Dagle

Pacific Northwest National Laboratory

(509) 375-3629

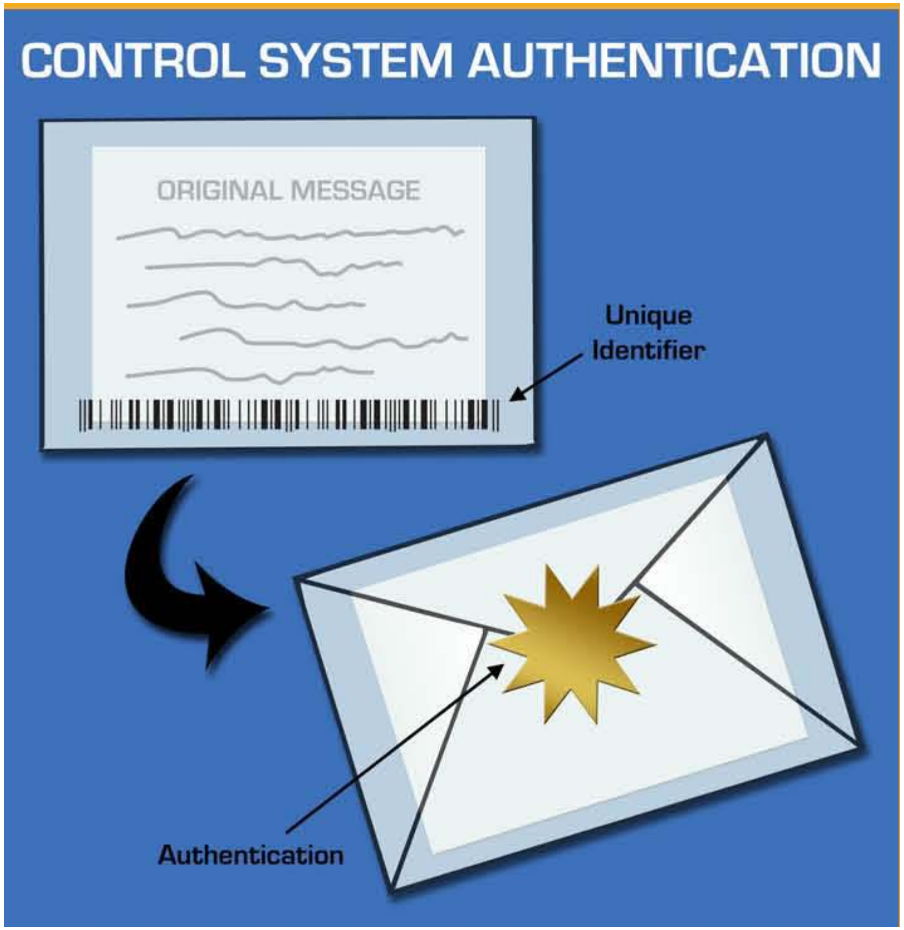
jeff.dagle@pnl.gov

The Pacific Northwest National Laboratory is a multiprogram laboratory operated by Battelle for the United States Department of Energy under contract DE-AC05-76RL01830.

U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

Work Package Description

- Leveraging prior investment by the Office of Naval Research through its National Center for Advanced Secure Systems Research, the NSTB will perform comprehensive testing to verify the integrity of the technical approach across a broad range of anticipated operating conditions
- **Primary Roadmap Goal:** Develop and integrate protective measures
- **Task budget:** $200K



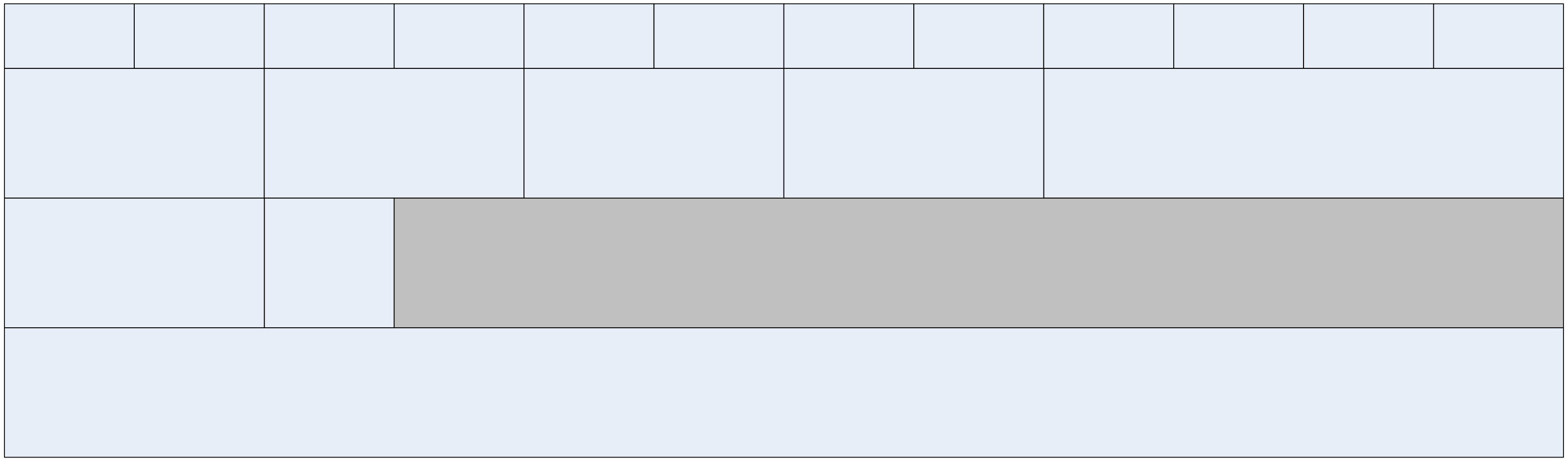
Technology goal: Ensure authentic communication while original message remains in clear text

Industry Needs

- Today, control system devices, protocols and communication media do not support the ability to adequately prevent cyber attacks against our critical infrastructure
- An environment of implicit trust is assumed
- Technology such as the cyclic redundancy check (CRC) is implemented to verify integrity of transmitted signals, protects against communication noise
- Protocol authenticator technology that operates in a similar mode could assure ***integrity*** of control and data acquisition signals, but without concerns introduced by full-signal encryption (e.g., latency, safety concerns, availability issues, etc.)
- Perfectly suited technology when ***confidentiality*** of the transmitted data is less important

The Technology

- Authenticate traffic using a hashed message authentication code (HMAC)
- Data remains in clear text
  - Ensures integrity of message, but also preserves safety, reliability
- Scalable technology that can be incorporated in new protocol divers (software) or “bump in the wire” retrofit (hardware) for legacy systems



Technical Approach

- Formed advisory board to guide research and development activities
  - Michael Assante, INL (formerly AEP)
  - Tom Flowers, CenterPoint Energy
  - Sam Jones, ERCOT
  - Scott Mix, NERC
- Began with notion of commercialization in mind
- Target protocol vendors for technology transfer
- Work with DNP Users Group and IEC TC57 WG15 to include message integrity in upcoming protocol standards (e.g., IEC-60870-5 and derivatives)

Technical Approach – cont.

- Embed software solution into end devices (SCADA Master/FEP or IED)
- SCADA message is “wrapped” with a unique identifier and an authenticator based upon the header and original message
- Each remote device has its own authentication key
- Two forms of key update have been implemented – Diffie Hellman and pre-shared
- Support for sha-1 or sha-256 for authenticator

Technical Progress - Accomplishments

- Progress from NCASSR Project:
  - Two year project
  - Prototype technology developed
  - Field tested at CenterPoint Energy
- NSTB Progress (FY06 new start, 58% expended as of 9/30)
  - Added support for Modbus to Windows code base
  - Added support for variable length authenticator to all platforms
  - Configuration GUI updated to support enhanced product
  - 50% complete with Linux version of code base
  - 25% complete with performance testing
  - Began discussions with SEL regarding technology transfer – looking to focus efforts on protocol vendors vs. hardware vendors
  - Plans to share protocol structure with IEC TC57 WG15 are in place
- Anticipated remaining schedule:
  - Baseline and performance testing complete 10/31/06
  - Cyber security testing complete 3/1/07
  - Final report 4/1/07

Industry Benefits

- Provide trusted control systems communication
- Embedded solution provides better performance than bump in the wire encryption devices
- Allows operators to continue to read and interpret telemetry data for troubleshooting purposes
- Key update and hash algorithms tailored to environment
- Supports both low and high-bandwidth environments